UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,568	10/24/2003	Woo-hyoung Lee	1572.1169	7526

21171 7590 04/06/2007

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
CUNNINGHAM, GREGORY F	
ART UNIT	PAPER NUMBER
2624	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,568	LEE, WOO-HYOUNG	
	Examiner	Art Unit	
	Greg F. Cunningham	2624	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications of application received 10/24/2003.

2. The disposition of the claims is as follows: claims 1 - 14 are pending in the application. Claims 1, 7 and 13 are independent claims.

3. The group and/or Art Unit location of your application has changed. To aid in the correlation of any papers for this application, all further correspondence should be directed to Group Art Unit 2624 (effective 03/07). Please be sure to use the most current art unit number on all correspondence to help us route your case and respond to you in a timely fashion.

4. When making claim amendments, the applicant is encouraged to consider the references in their entireties, including those portions that have not been cited by the examiner and their equivalents as they may most broadly and appropriately apply to any particular anticipated claim amendments.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-3, 7 and 8 are rejected under 35 U.S.C. 102(a) as being anticipated by Ben-Aissa (US 2005/0109836 A1).

A. Ben-Aissa anticipates claim 1, "A security system using fingerprints, comprising:

a fingerprint scan part creating a fingerprint image when a finger contacts the fingerprint scan part [para. 0107 at 'FIGS. 9A-9G illustrate typical screens that may appear on the display 21 of terminal 20 during the authentication procedure, which must be satisfactorily performed prior to obtaining access of any of the other available functions on terminal 20. The initial screen in FIG. 9A instructs the employee to place a finger on the fingerprint reader 30 of terminal 20. Use of a left finger on fingerprint reader 30 is preferable since it keeps the right hand conveniently available for making entries on keyboard 25 or on touch-sensitive screen 21. Of course, if fingerprint reader 30 was disposed on the right side of terminal 20, the opposite would be true, i.e., it would be preferable to read a right finger to keep the left hand available for keyboard or screen entries. When the employee is ready, he/she is instructed to actuate the fingerprint reader by touching the start button on the screen or by actuating the fingerprint reading key on the keyboard 25, as shown in FIG. 9B.'];

a fingerprint image storing part storing representative reference fingerprint images and at least one auxiliary reference fingerprint image for registered users [para. 0036 at 'In an initial registration process, the electronic terminal gathers biometric information, such as a fingerprint, which is then stored at the electronic terminal or in memory of the APW system for future comparison purposes.' and at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system.']; and

a control part determining whether one of the representative reference fingerprint images matches a first input fingerprint image input through the fingerprint scan part, reading auxiliary reference fingerprint images corresponding to a matching representative reference fingerprint

image, and comparing other fingerprint images input after the first input fingerprint image with the auxiliary reference fingerprint images to determine user authentication [para. 0107 at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system. The initial registration procedure, which captures images of the employee's fingerprints, is presented in greater detail below with reference to FIGS. 17A-17H. If the fingerprint reading is matched with a fingerprint on file, such as in a memory of terminal 20 or in the APW system, the next screen to appear on terminal 20 may be the screen in FIG. 9D requesting further information, such as an employee number, which may be a social security number, or requesting that the employee swipe his/her bankcard 23 in the slot of the bankcard reader 22. Note that in this example, the social security number or bankcard information is used to supplement the fingerprint identity, but some employers may be satisfied with only the use of the fingerprint verification or bankcard verification for purposes of check-in. Of course, if only bankcard verification is used for authentication on terminal 20, the employee may also be directed to enter a personal identification number associated with the bankcard number. After entering the social security number or swiping the bankcard, the employee presses the check or accept key on keypad 25 or on screen 21 to continue as shown in FIG. 9D. If only fingerprint identity is used for punching in, the authentication process may skip to the screen of FIG. 9E in which the employee is welcomed by his/her name and provided with various options for further action such as checking in or checking out of work.']" [as detailed].

B. Ben-Aissa anticipates claim 2, "The security system using fingerprints according to claim 1, wherein the control part displays an error message when the first input fingerprint image does

not match any of the representative reference fingerprint images in the fingerprint image storing part [para. 0108 at 'However, if terminal 20 cannot match the fingerprint from reader 30 with a corresponding image on file, the screen of FIG. 9C will appear advising of the inability to match the fingerprint. Preferably, there will be a side-by-side comparison of the closest print on file and the currently read image. Orthogonally disposed crosshairs 31 may indicate that the employee placed his/her finger too high or too low, or too far to the left or right, compared with the file image. Preferably, the origin of the crosshairs 31 will coincide near the center of the fingerprint image. Thus, the side-by-side images will assist the employee in attempting to get better centrally located placement of his/her finger on the next reading attempt.']" supra for claim 1 and [as detailed].

C. Ben-Aissa anticipates claim 3, "The security system using fingerprints according to claim 2, further comprising a fingerprint registering part sequentially storing fingerprint images input through the fingerprint scan part by an unregistered user in the fingerprint image storing part [Para. 0059 at 'FIGS. 17A-17H illustrate typical screens that may be used on the display of the electronic terminal of FIG. 1 to add or register new employees.'; para. 0131-0132 at 'FIGS. 17A-17H illustrate the procedure for registering a new employee, including obtaining useable fingerprint images from the new employee with the fingerprint reader 30 of terminal 20 for later use in the authentication procedures of FIGS. 9A-9G, above. This entails providing about three images of a finger, such as the left index finger, to the system for subsequent comparisons during future uses of the terminal 20. In FIG. 17A, a supervisor selects the Administration function by pressing the 5 key on keypad 25. In FIG. 17B, the supervisor selects the Register Employee function by pressing the 2 key on keypad 25. In the screen of FIG. 17C, the identity of the new

employee, such as an account number associated with bankcard 23, a social security number, or other employee number is entered via keypad 25. Such an employee ID number will be associated with fingerprint images by the APW system and/or terminal 20 in subsequent authentication procedures. When the employee ID number is entered and the check or accept box is actuated, the screen of FIG. 17D appears asking if the new employee is already registered on a different site or location. If so, fingerprint images already in the system may be used at the new work location. If not, the procedure continues to the screen of FIG. 17E.

In FIG. 17E, the new employee is then requested to capture a fingerprint image by placing a finger on the fingerprint reader 30, as in FIG. 9A. In the example of FIGS. 17A-17H, the new employee may a supervisor since supervisors must also register with the system in order to gain access thereto. Pressing of the fingerprint reader button captures the fingerprint image and displays it on the screen shown in FIG. 17F. The captured image is compared to acceptable and unacceptable images and the employee is prompted to decide whether to accept the captured image as a reference image for future comparison efforts during authentication procedures. As seen in FIG. 17F, the perfect image is one that is not too dark, nor too light, and which displays sufficient fingerprint detail. Preferably, the image of the fingerprint captures the whorl, and has differentiated ridge and valley areas with distinct lines of relatively high contrast. A poor image may be due to a dirty finger, placing the finger too high or too low on the reader 30, or using too much or too little pressure against the reader.'], and displaying the stored fingerprint images of the unregistered user for the unregistered user to select one of the stored fingerprint images as the representative reference fingerprint image [para. 0132 at 'Pressing of the fingerprint reader button captures the fingerprint image and displays it on the screen shown in FIG. 17F. The

captured image is compared to acceptable and unacceptable images and the employee is prompted to decide whether to accept the captured image as a reference image for future comparison efforts during authentication procedures.']" supra for claim 2 and [as detailed].

D. Ben-Aissa anticipates claim 7, "A security method using fingerprints, comprising:

storing representative reference fingerprint images and at least one auxiliary reference fingerprint image, according to registered users [para. 0107 at 'FIGS. 9A-9G illustrate typical screens that may appear on the display 21 of terminal 20 during the authentication procedure, which must be satisfactorily performed prior to obtaining access of any of the other available functions on terminal 20. The initial screen in FIG. 9A instructs the employee to place a finger on the fingerprint reader 30 of terminal 20. Use of a left finger on fingerprint reader 30 is preferable since it keeps the right hand conveniently available for making entries on keyboard 25 or on touch-sensitive screen 21. Of course, if fingerprint reader 30 was disposed on the right side of terminal 20, the opposite would be true, i.e., it would be preferable to read a right finger to keep the left hand available for keyboard or screen entries. When the employee is ready, he/she is instructed to actuate the fingerprint reader by touching the start button on the screen or by actuating the fingerprint reading key on the keyboard 25, as shown in FIG. 9B.'];

receiving a first input fingerprint image for authentication of a user [para. 0107 at 'when the employee was first registered on the APW system.'];

determining whether one of the stored representative reference fingerprint images matches the first input fingerprint image [para. 0107 at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system. The initial registration procedure, which captures

images of the employee's fingerprints, is presented in greater detail below with reference to FIGS. 17A-17H. If the fingerprint reading is matched with a fingerprint on file, such as in a memory of terminal 20 or in the APW system, the next screen to appear on terminal 20 may be the screen in FIG. 9D requesting further information, such as an employee number, which may be a social security number, or requesting that the employee swipe his/her bankcard 23 in the slot of the bankcard reader 22. Note that in this example, the social security number or bankcard information is used to supplement the fingerprint identity, but some employers may be satisfied with only the use of the fingerprint verification or bankcard verification for purposes of check-in. Of course, if only bankcard verification is used for authentication on terminal 20, the employee may also be directed to enter a personal identification number associated with the bankcard number. After entering the social security number or swiping the bankcard, the employee presses the check or accept key on keypad 25 or on screen 21 to continue as shown in FIG. 9D. If only fingerprint identity is used for punching in, the authentication process may skip to the screen of FIG. 9E in which the employee is welcomed by his/her name and provided with various options for further action such as checking in or checking out of work.'];

reading auxiliary reference fingerprint images corresponding to a matching representative reference fingerprint image [para. 0107 at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system. The initial registration procedure, which captures images of the employee's fingerprints, is presented in greater detail below with reference to FIGS. 17A-17H. If the fingerprint reading is matched with a fingerprint on file, such as in a memory of terminal 20 or in the APW system, the next screen to appear on terminal 20 may be the screen in FIG. 9D

requesting further information, such as an employee number, which may be a social security number, or requesting that the employee swipe his/her bankcard 23 in the slot of the bankcard reader 22. Note that in this example, the social security number or bankcard information is used to supplement the fingerprint identity, but some employers may be satisfied with only the use of the fingerprint verification or bankcard verification for purposes of check-in. Of course, if only bankcard verification is used for authentication on terminal 20, the employee may also be directed to enter a personal identification number associated with the bankcard number. After entering the social security number or swiping the bankcard, the employee presses the check or accept key on keypad 25 or on screen 21 to continue as shown in FIG. 9D. If only fingerprint identity is used for punching in, the authentication process may skip to the screen of FIG. 9E in which the employee is welcomed by his/her name and provided with various options for further action such as checking in or checking out of work.'];

receiving additional fingerprint images sequentially input by the user [Para. 0059 at 'FIGS. 17A-17H illustrate typical screens that may be used on the display of the electronic terminal of FIG. 1 to add or register new employees.'; para. 0131-0132 at 'FIGS. 17A-17H illustrate the procedure for registering a new employee, including obtaining useable fingerprint images from the new employee with the fingerprint reader 30 of terminal 20 for later use in the authentication procedures of FIGS. 9A-9G, above. This entails providing about three images of a finger, such as the left index finger, to the system for subsequent comparisons during future uses of the terminal 20. In FIG. 17A, a supervisor selects the Administration function by pressing the 5 key on keypad 25. In FIG. 17B, the supervisor selects the Register Employee function by pressing the 2 key on keypad 25. In the screen of FIG. 17C, the identity of the new employee, such as an

account number associated with bankcard 23, a social security number, or other employee number is entered via keypad 25. Such an employee ID number will be associated with fingerprint images by the APW system and/or terminal 20 in subsequent authentication procedures. When the employee ID number is entered and the check or accept box is actuated, the screen of FIG. 17D appears asking if the new employee is already registered on a different site or location. If so, fingerprint images already in the system may be used at the new work location. If not, the procedure continues to the screen of FIG. 17E.

In FIG. 17E, the new employee is then requested to capture a fingerprint image by placing a finger on the fingerprint reader 30, as in FIG. 9A. In the example of FIGS. 17A-17H, the new employee may a supervisor since supervisors must also register with the system in order to gain access thereto. Pressing of the fingerprint reader button captures the fingerprint image and displays it on the screen shown in FIG. 17F. The captured image is compared to acceptable and unacceptable images and the employee is prompted to decide whether to accept the captured image as a reference image for future comparison efforts during authentication procedures. As seen in FIG. 17F, the perfect image is one that is not too dark, nor too light, and which displays sufficient fingerprint detail. Preferably, the image of the fingerprint captures the whorl, and has differentiated ridge and valley areas with distinct lines of relatively high contrast. A poor image may be due to a dirty finger, placing the finger too high or too low on the reader 30, or using too much or too little pressure against the reader.']; and

determining whether the user is authenticated by respectively comparing the additional input fingerprint images with the corresponding auxiliary reference fingerprint images [para. 0107 at 'The initial registration procedure, which captures images of the employee's fingerprints,

is presented in greater detail below with reference to FIGS. 17A-17H. If the fingerprint reading is matched with a fingerprint on file, such as in a memory of terminal 20 or in the APW system, the next screen to appear on terminal 20 may be the screen in FIG. 9D requesting further information, such as an employee number, which may be a social security number, or requesting that the employee swipe his/her bankcard 23 in the slot of the bankcard reader 22. Note that in this example, the social security number or bankcard information is used to supplement the fingerprint identity, but some employers may be satisfied with only the use of the fingerprint verification or bankcard verification for purposes of check-in. Of course, if only bankcard verification is used for authentication on terminal 20, the employee may also be directed to enter a personal identification number associated with the bankcard number. After entering the social security number or swiping the bankcard, the employee presses the check or accept key on keypad 25 or on screen 21 to continue as shown in FIG. 9D. If only fingerprint identity is used for punching in, the authentication process may skip to the screen of FIG. 9E in which the employee is welcomed by his/her name and provided with various options for further action such as checking in or checking out of work.']" [as detailed].

E. Ben-Aissa anticipates claim 8, "The security method using fingerprints according to claim 7, further comprising displaying an error message when the first input fingerprint image does not match any of the representative reference fingerprint images [para. 0108 at 'However, if terminal 20 cannot match the fingerprint from reader 30 with a corresponding image on file, the screen of FIG. 9C will appear advising of the inability to match the fingerprint. Preferably, there will be a side-by-side comparison of the closest print on file and the currently read image. Orthogonally disposed crosshairs 31 may indicate that the employee placed his/her finger too

high or too low, or too far to the left or right, compared with the file image. Preferably, the origin of the crosshairs 31 will coincide near the center of the fingerprint image. Thus, the side-by-side images will assist the employee in attempting to get better centrally located placement of his/her finger on the next reading attempt.']" supra for claim 7 and [as detailed].

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 4-6, 9-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ben-Aissa as applied to claim 3 above, and further in view of Bergstrom (US 2002/0122026 A1).

A. Ben-Aissa discloses claim 4, "The security system using fingerprints according to claim 3, wherein the fingerprint registering part assigns sequential order values to the unregistered fingerprint images input through the fingerprint scan part and stores the sequential order values with the input fingerprint images of the unregistered user in the fingerprint image storing part" supra for claim 3. However Ben-Aissa does not appear to disclose "wherein the fingerprint registering part assigns sequential order values to the unregistered fingerprint images input through the fingerprint scan part and stores the sequential order values with the input fingerprint images of the unregistered user in the fingerprint image storing part", but Bergstrom does in [para. 0026 at 'The fingerprint interpreter 415 generates a sequence of characteristic data ("fingerprint map") that represents the sensed fingerprint image. The identity verification system

435 in the computer 405 reads the fingerprint map and determines whether the fingerprint map matches a stored reference fingerprint image. The two-dimensional position interpreter 420 generates an x-y coordinate position of the center of the fingerprint map on the contact surface 22. In one preferred embodiment, the coordinate position is determined by computing the arithmetic center of mass for the fingerprint map. The mouse driver program 440 reads the x-y coordinate position and uses the information to control the position of a visual cue on a display screen. The embodiment shown in FIG. 4 is meant to be exemplary and variations thereof would be apparent to one skilled in the art.', where 'a sequence of characteristic ("fingerprint map")' corresponds to "assigns sequential order values to the unregistered fingerprint images input".]

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

B. Ben-Aissa discloses claim 5, "The security system using fingerprints according to claim 3, wherein the fingerprint scan part comprises multiple fingerprint input keys having order values sequentially selected by the unregistered user; and the fingerprint registering part stores a combination of input fingerprint images contacting the fingerprint input keys selected by the unregistered user and the order values in the fingerprint image storing part" supra for claim 3.

However Ben-Aissa does not appear to disclose "wherein the fingerprint scan part comprises multiple fingerprint input keys having order values sequentially selected by the

unregistered user [Bergstrom - para. 0026 at 'The information furnished by the fingerprint scanner 410 consists of a high resolution bit map of the surface of the fingerprint touch pad 400. The fingerprint interpreter 415 generates a sequence of characteristic data ("fingerprint map") that represents the sensed fingerprint image.']; and the fingerprint registering part stores a combination of input fingerprint images contacting the fingerprint input keys selected by the unregistered user and the order values in the fingerprint image storing part [Bergstrom - para. 0023 at 'In one preferred embodiment, the fingerprint image is stored in a memory 315.' and para. 0025 at 'In an alternate embodiment of the invention, the primary purpose of the security system might not be to limit or prevent access to all or part of a system, but rather to record who has had access to the system. In this embodiment, after the fingerprint has been identified 310, as shown in FIG. 3, the identification is stored in memory 315.']", but Bergstrom does [Bergstrom - as detailed].

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") and fingerprint touchpad disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

C. Ben-Aissa and Bergstrom disclose claim 6, "The security system using fingerprints according to claim 4, wherein the fingerprint registering part displays a screen to set the input order of the auxiliary reference fingerprint images [Bergstrom – para. 0018 at 'In one preferred embodiment, the contact surface includes sensors of a type capable of sensing both a coordinate

position and a fingerprint image. A processor receives the sensed coordinate position information 24 and causes the cursor 28 to appear in a correlated position on the display 30 of a computer. The processor receives the sensed fingerprint image 26 and compares it to stored reference fingerprint images. If the sensed image matches a stored reference image, access to the computer is allowed.', wherein 'coordinate position information 24 and causes the cursor 28 to appear in a correlated position on the display 30' corresponds to "displays a screen to set the input order of the auxiliary reference fingerprint images"]; and the control part stores the input order of the auxiliary reference fingerprint images in the fingerprint image storing part [Bergstrom – para. 0023 at 'In one preferred embodiment, the fingerprint image is stored in a memory 315.']" supra for claim 4 and [as detailed].

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") and coordinate and correlated position disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

D. Ben-Aissa and Bergstrom disclose claim 9, "The security method using fingerprints according to claim 8, further comprising:

receiving fingerprint images of an unregistered user [Ben-Aissa - Para. 0059 at 'FIGS. 17A-17H illustrate typical screens that may be used on the display of the electronic terminal of FIG. 1 to add or register new employees.'; para. 0131-0132 at 'FIGS. 17A-17H illustrate the procedure for registering a new employee, including obtaining useable fingerprint images from

the new employee with the fingerprint reader 30 of terminal 20 for later use in the authentication procedures of FIGS. 9A-9G, above. This entails providing about three images of a finger, such as the left index finger, to the system for subsequent comparisons during future uses of the terminal 20. In FIG. 17A, a supervisor selects the Administration function by pressing the 5 key on keypad 25. In FIG. 17B, the supervisor selects the Register Employee function by pressing the 2 key on keypad 25. In the screen of FIG. 17C, the identity of the new employee, such as an account number associated with bankcard 23, a social security number, or other employee number is entered via keypad 25. Such an employee ID number will be associated with fingerprint images by the APW system and/or terminal 20 in subsequent authentication procedures. When the employee ID number is entered and the check or accept box is actuated, the screen of FIG. 17D appears asking if the new employee is already registered on a different site or location. If so, fingerprint images already in the system may be used at the new work location. If not, the procedure continues to the screen of FIG. 17E.

In FIG. 17E, the new employee is then requested to capture a fingerprint image by placing a finger on the fingerprint reader 30, as in FIG. 9A. In the example of FIGS. 17A-17H, the new employee may a supervisor since supervisors must also register with the system in order to gain access thereto. Pressing of the fingerprint reader button captures the fingerprint image and displays it on the screen shown in FIG. 17F. The captured image is compared to acceptable and unacceptable images and the employee is prompted to decide whether to accept the captured image as a reference image for future comparison efforts during authentication procedures. As seen in FIG. 17F, the perfect image is one that is not too dark, nor too light, and which displays sufficient fingerprint detail. Preferably, the image of the fingerprint captures the whorl, and has

differentiated ridge and valley areas with distinct lines of relatively high contrast. A poor image may be due to a dirty finger, placing the finger too high or too low on the reader 30, or using too much or too little pressure against the reader.']; and

assigning order values to the fingerprint images sequentially input by the unregistered user, and storing the order values with the input fingerprint images [Bergstrom - para. 0026 at 'The fingerprint interpreter 415 generates a sequence of characteristic data ("fingerprint map") that represents the sensed fingerprint image. The identity verification system 435 in the computer 405 reads the fingerprint map and determines whether the fingerprint map matches a stored reference fingerprint image. The two-dimensional position interpreter 420 generates an x-y coordinate position of the center of the fingerprint map on the contact surface 22. In one preferred embodiment, the coordinate position is determined by computing the arithmetic center of mass for the fingerprint map. The mouse driver program 440 reads the x-y coordinate position and uses the information to control the position of a visual cue on a display screen. The embodiment shown in FIG. 4 is meant to be exemplary and variations thereof would be apparent to one skilled in the art.', where 'a sequence of characteristic ("fingerprint map")' corresponds to "assigns sequential order values to the unregistered fingerprint images input".]" supra for claim 8 and [as detailed].

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification

purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

E. Ben-Aissa and Bergstrom disclose claim 10, "The security method using fingerprints according to claim 9, further comprising displaying a screen for the unregistered user to select one of the stored representative reference fingerprint images as the representative reference fingerprint image [Ben-Aissa - para. 0132 at 'Pressing of the fingerprint reader button captures the fingerprint image and displays it on the screen shown in FIG. 17F. The captured image is compared to acceptable and unacceptable images and the employee is prompted to decide whether to accept the captured image as a reference image for future comparison efforts during authentication procedures.']" supra for claim 9 and [as detailed].

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

F. Ben-Aissa and Bergstrom disclose claim 11, "The security method using fingerprints according to claim 10, further comprising:

displaying a screen to select and assign order values to the auxiliary reference fingerprint images [Bergstrom - Bergstrom – para. 0018 at 'In one preferred embodiment, the contact surface includes sensors of a type capable of sensing both a coordinate position and a fingerprint image. A processor receives the sensed coordinate position information 24 and causes the cursor

28 to appear in a correlated position on the display 30 of a computer. The processor receives the sensed fingerprint image 26 and compares it to stored reference fingerprint images. If the sensed image matches a stored reference image, access to the computer is allowed.', wherein 'coordinate position information 24 and causes the cursor 28 to appear in a correlated position on the display 30' corresponds to "displays a screen to set the input order of the auxiliary reference fingerprint images"]; and

storing the selected auxiliary reference fingerprint image and the order values with the selected representative reference fingerprint image [Bergstrom – para. 0023 at 'In one preferred embodiment, the fingerprint image is stored in a memory 315.']" supra for claim 10 and [as detailed].

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") and coordinate and correlated position disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

G. Ben-Aissa and Bergstrom disclose claim 12, "The security method using fingerprints according to claim 8, further comprising:

selecting sequentially two or more fingerprint input keys having order values selected by the unregistered user [Ben-Aissa - Para. 0059 at 'FIGS. 17A-17H illustrate typical screens that may be used on the display of the electronic terminal of FIG. 1 to add or register new employees.'; para. 0131-0132 at 'FIGS. 17A-17H illustrate the procedure for registering a new employee,

including obtaining useable fingerprint images from the new employee with the fingerprint reader 30 of terminal 20 for later use in the authentication procedures of FIGS. 9A-9G, above. This entails providing about three images of a finger, such as the left index finger, to the system for subsequent comparisons during future uses of the terminal 20. In FIG. 17A, a supervisor selects the Administration function by pressing the 5 key on keypad 25. In FIG. 17B, the supervisor selects the Register Employee function by pressing the 2 key on keypad 25. In the screen of FIG. 17C, the identity of the new employee, such as an account number associated with bankcard 23, a social security number, or other employee number is entered via keypad 25. Such an employee ID number will be associated with fingerprint images by the APW system and/or terminal 20 in subsequent authentication procedures. When the employee ID number is entered and the check or accept box is actuated, the screen of FIG. 17D appears asking if the new employee is already registered on a different site or location. If so, fingerprint images already in the system may be used at the new work location. If not, the procedure continues to the screen of FIG. 17E.

In FIG. 17E, the new employee is then requested to capture a fingerprint image by placing a finger on the fingerprint reader 30, as in FIG. 9A. In the example of FIGS. 17A-17H, the new employee may a supervisor since supervisors must also register with the system in order to gain access thereto. Pressing of the fingerprint reader button captures the fingerprint image and displays it on the screen shown in FIG. 17F. The captured image is compared to acceptable and unacceptable images and the employee is prompted to decide whether to accept the captured image as a reference image for future comparison efforts during authentication procedures. As seen in FIG. 17F, the perfect image is one that is not too dark, nor too light, and which displays

sufficient fingerprint detail. Preferably, the image of the fingerprint captures the whorl, and has differentiated ridge and valley areas with distinct lines of relatively high contrast. A poor image may be due to a dirty finger, placing the finger too high or too low on the reader 30, or using too much or too little pressure against the reader.'];

storing a combination of fingerprint images input through the selected fingerprint input keys and the order values [Ben-Aissa - para. 0036 at 'In an initial registration process, the electronic terminal gathers biometric information, such as a fingerprint, which is then stored at the electronic terminal or in memory of the APW system for future comparison purposes.' and at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system.']; and

determining authentication of a user requesting authentication by determining whether an order of the fingerprint images input through the fingerprint input keys matches the selected order values and whether the input fingerprint images match the stored auxiliary reference fingerprint images [Ben-Aissa - para. 0107 at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system. The initial registration procedure, which captures images of the employee's fingerprints, is presented in greater detail below with reference to FIGS. 17A-17H. If the fingerprint reading is matched with a fingerprint on file, such as in a memory of terminal 20 or in the APW system, the next screen to appear on terminal 20 may be the screen in FIG. 9D requesting further information, such as an employee number, which may be a social security number, or requesting that the employee swipe his/her bankcard 23 in the slot of the bankcard reader 22. Note that in this example, the social security number or bankcard information is used

to supplement the fingerprint identity, but some employers may be satisfied with only the use of the fingerprint verification or bankcard verification for purposes of check-in. Of course, if only bankcard verification is used for authentication on terminal 20, the employee may also be directed to enter a personal identification number associated with the bankcard number. After entering the social security number or swiping the bankcard, the employee presses the check or accept key on keypad 25 or on screen 21 to continue as shown in FIG. 9D. If only fingerprint identity is used for punching in, the authentication process may skip to the screen of FIG. 9E in which the employee is welcomed by his/her name and provided with various options for further action such as checking in or checking out of work.']" supra for claim 8 and [as detailed].

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") and coordinate and correlated position disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

H. Ben-Aissa and Bergstrom disclose claim 13, "A fingerprint security method, comprising:

receiving and storing fingerprint images for each finger of one or more unregistered users [since Ben-Aissa and Bergstrom demonstrate fingerprint images for at least one finger, supra, it would be obvious to do the same for each finger];

displaying the stored fingerprint images for the unregistered user to select one of the stored fingerprint images as a representative reference fingerprint image [Ben-Aissa - para. 0132 at 'Pressing of the fingerprint reader button captures the fingerprint image and displays it on the

screen shown in FIG. 17F. The captured image is compared to acceptable and unacceptable images and the employee is prompted to decide whether to accept the captured image as a reference image for future comparison efforts during authentication procedures.'];

displaying the stored fingerprint images for the unregistered user to select and order one or more of the stored fingerprint images as ordered auxiliary reference fingerprint images [Ben-Aissa - para. 0026 at 'The fingerprint interpreter 415 generates a sequence of characteristic data ("fingerprint map") that represents the sensed fingerprint image. The identity verification system 435 in the computer 405 reads the fingerprint map and determines whether the fingerprint map matches a stored reference fingerprint image. The two-dimensional position interpreter 420 generates an x-y coordinate position of the center of the fingerprint map on the contact surface 22. In one preferred embodiment, the coordinate position is determined by computing the arithmetic center of mass for the fingerprint map. The mouse driver program 440 reads the x-y coordinate position and uses the information to control the position of a visual cue on a display screen. The embodiment shown in FIG. 4 is meant to be exemplary and variations thereof would be apparent to one skilled in the art.', where 'a sequence of characteristic ("fingerprint map")' corresponds to "assigns sequential order values to the unregistered fingerprint images input".];

registering the user with the corresponding representative reference fingerprint image and the auxiliary reference fingerprint images [Ben-Aissa – para. 0036 at 'Access to the system is permitted after authentication by a biometric device, such as a fingerprint reader, or by a bankcard and a personal identification number (PIN). In an initial registration process, the electronic terminal gathers biometric information, such as a fingerprint, which is then stored at the electronic terminal or in memory of the APW system for future comparison purposes.'];

receiving a first fingerprint image from a user to be authenticated [Ben-Aissa - para. 0036 at 'In an initial registration process, the electronic terminal gathers biometric information, such as a fingerprint, which is then stored at the electronic terminal or in memory of the APW system for future comparison purposes.' and at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system.'];

determining whether the first fingerprint image matches any of a plurality of stored representative reference fingerprint images for a plurality of registered users [Ben-Aissa - para. 0107 at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system. The initial registration procedure, which captures images of the employee's fingerprints, is presented in greater detail below with reference to FIGS. 17A-17H. If the fingerprint reading is matched with a fingerprint on file, such as in a memory of terminal 20 or in the APW system, the next screen to appear on terminal 20 may be the screen in FIG. 9D requesting further information, such as an employee number, which may be a social security number, or requesting that the employee swipe his/her bankcard 23 in the slot of the bankcard reader 22. Note that in this example, the social security number or bankcard information is used to supplement the fingerprint identity, but some employers may be satisfied with only the use of the fingerprint verification or bankcard verification for purposes of check-in. Of course, if only bankcard verification is used for authentication on terminal 20, the employee may also be directed to enter a personal identification number associated with the bankcard number. After entering the social security number or swiping the bankcard, the employee presses the check or accept key on keypad 25 or

on screen 21 to continue as shown in FIG. 9D. If only fingerprint identity is used for punching in, the authentication process may skip to the screen of FIG. 9E in which the employee is welcomed by his/her name and provided with various options for further action such as checking in or checking out of work.'];

receiving, when the first fingerprint image matches one of the stored representative reference fingerprint images, additional fingerprint images sequentially input by the user to be authenticated [Bergstrom – para. 0026 – 0027 at 'FIG. 4 shows a block diagram of a fingerprint touch pad 400 and a computer 405. A fingerprint interpreter 415 and a two-dimensional position interpreter 420 read information from a fingerprint scanner 410. The information furnished by the fingerprint scanner 410 consists of a high resolution bit map of the surface of the fingerprint touch pad 400. The fingerprint interpreter 415 generates a sequence of characteristic data ("fingerprint map") that represents the sensed fingerprint image. The identity verification system 435 in the computer 405 reads the fingerprint map and determines whether the fingerprint map matches a stored reference fingerprint image. The two-dimensional position interpreter 420 generates an x-y coordinate position of the center of the fingerprint map on the contact surface 22. In one preferred embodiment, the coordinate position is determined by computing the arithmetic center of mass for the fingerprint map. The mouse driver program 440 reads the x-y coordinate position and uses the information to control the position of a visual cue on a display screen. The embodiment shown in FIG. 4 is meant to be exemplary and variations thereof would be apparent to one skilled in the art.

[0027] It should be noted that although the present invention may be used to control a cursor as a visual display, an alternate embodiment does not include the visual display. This

embodiment might be used for a "signing security" system in which a user uses his finger to sign his name on a touch pad. The system would verify both the fingerprint and the signature. No visual display, however, would be necessary.']; and

determining whether each of the additional fingerprint images matches auxiliary reference fingerprint images corresponding to the representative reference fingerprint image that matches the first fingerprint image, and whether the additional fingerprint images are input according to the selected order of the corresponding auxiliary reference fingerprint images [Ben-Aissa - para. 0107 at 'Terminal 20 then compares the fingerprint from fingerprint reader 30 with fingerprints scans that were made when the employee was first registered on the APW system. The initial registration procedure, which captures images of the employee's fingerprints, is presented in greater detail below with reference to FIGS. 17A-17H. If the fingerprint reading is matched with a fingerprint on file, such as in a memory of terminal 20 or in the APW system, the next screen to appear on terminal 20 may be the screen in FIG. 9D requesting further information, such as an employee number, which may be a social security number, or requesting that the employee swipe his/her bankcard 23 in the slot of the bankcard reader 22. Note that in this example, the social security number or bankcard information is used to supplement the fingerprint identity, but some employers may be satisfied with only the use of the fingerprint verification or bankcard verification for purposes of check-in. Of course, if only bankcard verification is used for authentication on terminal 20, the employee may also be directed to enter a personal identification number associated with the bankcard number. After entering the social security number or swiping the bankcard, the employee presses the check or accept key on keypad 25 or on screen 21 to continue as shown in FIG. 9D. If only fingerprint identity is used

for punching in, the authentication process may skip to the screen of FIG. 9E in which the employee is welcomed by his/her name and provided with various options for further action such as checking in or checking out of work.']" [as detailed.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") and coordinate and correlated position disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

J. Ben-Aissa and Bergstrom disclose claim 14, "The fingerprint security method according to claim 13, further comprising displaying an error message when the first input fingerprint image does not match any of the representative reference fingerprint images [Ben-Aissa - para. 0108 at 'However, if terminal 20 cannot match the fingerprint from reader 30 with a corresponding image on file, the screen of FIG. 9C will appear advising of the inability to match the fingerprint. Preferably, there will be a side-by-side comparison of the closest print on file and the currently read image. Orthogonally disposed crosshairs 31 may indicate that the employee placed his/her finger too high or too low, or too far to the left or right, compared with the file image. Preferably, the origin of the crosshairs 31 will coincide near the center of the fingerprint image. Thus, the side-by-side images will assist the employee in attempting to get better centrally located placement of his/her finger on the next reading attempt.']" supra for claim 13 and [as detailed].

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply fingerprint scanner reader disclosed by Ben-Aissa in combination with characteristic ("fingerprint map") and coordinate and correlated position disclosed by Bergstrom, and motivated to combine the teachings because it would "performs both fingerprint sensing and matching for identification purposes, and controls the position of a cursor on a display screen for data input purposes" as revealed by Bergstrom in para. 0010.

Responses

9. Responses to this action should be mailed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Inquiries

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory F. Cunningham whose telephone number is (571) 272-7784.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matt Bella can be reached on (571) 272-7778. The Central FAX Number for the organization where this application or proceeding is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

G.F. Cunningham

Gregory F. Cunningham
Examiner, Art Unit 2624

gfc

04/01/2007

Matthew C. Bella

MATTHEW C. BELLA
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600